ABSTRACT

An external module loads into an entity's memory and is transformed by two functions. These are namely, the STOMP function and the UNSTOMP function. One or both of these functions is based on the actual code that is found in a legitimate version of the external module. The STOMP-UNSTOMP pair produces an external module that works differently if even a single byte of code in the external module has been changed by an attacker. The STOMP transforms the external module and makes it temporarily unusable whilst conversely, the UNSTOMP repairs the damage and makes it workable again. Thus, if the module is not authentic, the pairing between the STOMP and UNSTOMP is broken. Therefore, a patched module from a hacker remains unusable since the STOMP and UNSTOMP transformations do not produce a working external module. Because of the STOMP and UNSTOMP technique, an application is secure because if an external module is free from tampering then the application executes normally. In the event that an illicitly patched external module is loaded then the application fails. In either case, no audio, video or information content is illegally copied because of the disablement of the external module by the STOMP-UNSTOMP procedure.